CYBER THREAT INTELLIGENCE, INCIDENT RESPONSE AND DIGITAL FORENSICS COURSE

Introduction

The Cyber Threat Intelligence, Incident Response and Digital Forensics Course is designed to equip cybersecurity professionals, ICT specialists, incident handlers, investigators and risk practitioners with the knowledge and practical skills required to identify cyber threats, investigate security incidents and coordinate effective responses. Organisations face increasingly sophisticated threats involving phishing, ransomware, compromised credentials, malicious software, insider activity and attacks against critical systems. An effective response depends on the ability to recognize warning signs, collect reliable evidence, understand the scope of compromise, contain the incident and restore operations without unnecessarily destroying information that may be needed for investigation, legal proceedings or regulatory reporting. The programme brings together three complementary disciplines. Cyber threat intelligence focuses on understanding threat actors, their capabilities, motivations, indicators and likely targets. Incident response focuses on the structured management of security events, from initial detection and triage through containment, eradication, recovery and lessons learned. Digital forensics focuses on the lawful and technically sound collection, preservation, examination and reporting of digital evidence. Participants examine security monitoring, threat intelligence sources, attack indicators, incident classification, evidence integrity, investigation documentation and post-incident improvement. The course also addresses coordination among technical teams, management, legal advisers, law enforcement and relevant external stakeholders. Through scenario-based exercises, participants develop incident response procedures, practise investigation planning and prepare incident reports.

Course Objectives

- Explain the principles and sources of cyber threat intelligence.
- Identify common attack patterns, indicators of compromise and suspicious activity.
- Apply structured procedures for incident detection, classification and triage.
- Develop incident response playbooks for common cybersecurity scenarios.
- Coordinate containment, eradication and recovery activities.
- Apply digital evidence preservation and chain-of-custody principles.
- Explain basic forensic examination of files, system logs and relevant digital artefacts.
- Document findings accurately and prepare evidence-based incident reports.
- Coordinate technical, management, legal and external stakeholder responses.
- Develop incident response improvement plans based on lessons learned.

Course Modules

> Module 1: Cyber Threat Intelligence Fundamentals
- Meaning, purpose and lifecycle of cyber threat intelligence.
- Strategic, operational, tactical and technical intelligence.
- Threat actors, motivations, capabilities and target selection.
- Intelligence requirements and prioritisation of organisational threats.

> Module 2: Threat Intelligence Sources and Analysis
- Open-source intelligence and reputable threat information sources.
- Indicators of compromise and indicators of attack.
- Threat intelligence feeds, sharing platforms and information quality.
- Analysing relevance, confidence, timeliness and potential business impact.

> Module 3: Cyberattack Patterns and Threat Detection
- Phishing, credential theft, ransomware and malicious software.
- Network, endpoint, identity and cloud security indicators.
- Introduction to attack frameworks such as MITRE ATT&CK.
- Recognizing suspicious events and distinguishing alerts from confirmed incidents.

> Module 4: Incident Response Planning and Readiness
- Incident response policies, procedures and escalation arrangements.
- Defining incident roles, responsibilities and communication channels.
- Incident classification, severity levels and response priorities.
- Developing playbooks for data breaches, malware and account compromise.

> Module 5: Incident Detection, Triage and Investigation
- Collecting and reviewing relevant logs and security alerts.
- Establishing incident timelines and identifying affected assets.
- Assessing scope, impact, persistence and potential data exposure.
- Documenting initial findings and preserving relevant evidence.

> Module 6: Containment, Eradication and Recovery
- Selecting proportionate containment measures.
- Isolating affected systems and protecting unaffected environments.
- Removing malicious artefacts and addressing the underlying cause.
- Validating system recovery and monitoring for recurrence

> Module 7: Digital Forensics and Evidence Preservation
- Principles, scope and limitations of digital forensic examination.
- Evidence identification, collection and preservation.
- Chain of custody, evidence integrity and documentation.
- Legal, ethical and organisational requirements for digital investigations.

> Module 8: Practical Forensic Examination and Reporting
- Introduction to file systems, metadata and digital artefacts.
- Examination of system logs, event records and relevant timestamps.
- Building timelines and correlating evidence from different sources.
- Preparing forensic notes, findings and structured investigation reports.

> Module 9: Incident Communication and Post-Incident Review
- Communicating technical findings to management and other stakeholders.
- Coordination with legal advisers, regulators and law enforcement where appropriate.
- Conducting root-cause analysis and assessing control failures.
- Lessons learned, corrective actions and incident response improvement.

> Module 10: Threat Intelligence and Incident Response Capstone
- Analysing a simulated security incident using supplied evidence.
- Developing a threat assessment and incident timeline.
- Preparing a response plan with containment and recovery priorities.
- Presenting an investigation report and recommendations for prevention.

P.O Box 7254- 01000
www.trustgatecorporateskills.co.ke
Location Thika & Nairobi